

On the complementary quantum capacity of the depolarizing channel

Debbie Leung*

John Watrous[†]

5 October, 2015

Abstract

The qubit depolarizing channel with noise parameter η transmits an input qubit perfectly with probability $1 - \eta$, and outputs the completely mixed state with probability η . We show that its *complementary channel* has *positive* quantum capacity for all $\eta > 0$. Thus, we find that there exists a single parameter family of channels having the peculiar property of having positive quantum capacity even when the outputs of these channels approach a fixed state independent of the input. Comparisons with other related channels, and implications on the difficulty of studying the quantum capacity of the depolarizing channel are discussed.

Introduction

It is a fundamental problem in quantum information theory to determine the capacity of quantum channels to transmit quantum information. The *quantum capacity* of a channel is the optimal rate at which one can transmit quantum data with high fidelity through that channel when an asymptotically large number of channel uses is made available.

In the classical setting, the capacity of a classical channel to transmit classical data is given by Shannon's noisy coding theorem [Sha48]. Although the error correcting codes that allow one to approach the capacity of a channel may involve increasingly large block lengths, the capacity expression itself is a simple, *single letter formula* involving an optimization over input distributions maximizing the input/output mutual information over *one* use of the channel.

In the quantum setting, analyses inspired by the classical setting have been performed [Llo97, Sho02, Dev05], and an expression for the quantum capacity has been found. However, the capacity expression involves an optimization similar to the classical setting not for a single channel use, but for an increasingly large number of channel uses. The optimum value for n copies of the channel leads to the so-called *n -shot coherent information* of the channel, but little is known in general about how the n -shot coherent information grows with n . (Reference [DSS98] showed that the

*Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo

[†]Institute for Quantum Computing and School of Computer Science, University of Waterloo

coherent information can be superadditive for some channels, so the one-shot coherent information does not generally provide an expression for the quantum capacity of a quantum channel.) Consequently, the quantum capacity is unknown for many quantum channels of interest.

Furthermore, [DSS98] showed that the n -shot coherent information of a channel can increase from zero to a positive quantity as n increases, and reference [CEM⁺15] showed that given any positive integer n , there is a channel whose n -shot coherent information is zero but whose quantum capacity is nevertheless positive. Moreover, no algorithm is known to determine if a quantum channel has zero or positive quantum capacity. On the other hand, some partial characterizations are known [BDS97, BDE⁺98, Per96, HHH00, SS12]. For several well-known families of quantum channels that can be characterized by noise parameters, the quantum capacity is proved to be zero within moderately noisy regimes, well before the channel output becomes constant and independent of the input.

In this paper, we show that any complementary channel to the qubit depolarizing channel has positive quantum capacity (in fact, positive one-shot coherent information) unless the output is exactly constant. This is in sharp contrast with the superficially similar qubit depolarizing channel and erasure channel, whose capacities vanish when the analogous noise parameter is roughly half-way between the completely noiseless and noisy extremes. Prior to this work, it was not known (to our knowledge) that a family of quantum channels could retain positive quantum capacity while approaching a channel whose output is a fixed state, independent of the channel input. We hope this example concerning how the quantum capacity does not vanish will shed light on a better characterization of when a channel has no quantum capacity.

Another consequence of our result concerns the quantum capacity of low-noise depolarizing channels. Watanabe [Wat12] showed that if a given channel's complementary channels have no quantum capacity, then the original channel must have quantum capacity equal to its private classical capacity. Furthermore, if the complementary channels have no classical private capacity, then the quantum and private capacities are given by the one-shot coherent information. Our result shows that Watanabe's results cannot be applied to the qubit depolarizing channel (although whether or not the conclusion holds remains open).

In the remainder of the paper, we review background information concerning quantum channels, quantum capacities, and relevant results on a few commonly studied families of channels, and then prove our main results.

Preliminaries

Given a sender (Alice) and a receiver (Bob), one typically models quantum communication from Alice to Bob as being sent through a quantum channel Φ . We will associate the input and output systems with finite-dimensional complex Hilbert spaces \mathcal{A} and \mathcal{B} , respectively. In general, we write $\mathcal{L}(\mathcal{X}, \mathcal{Y})$ to denote the space of linear operators from \mathcal{X} to \mathcal{Y} , for finite-dimensional complex Hilbert spaces \mathcal{X} and \mathcal{Y} , and we write $\mathcal{L}(\mathcal{X})$ to denote $\mathcal{L}(\mathcal{X}, \mathcal{X})$. We also write $\mathcal{D}(\mathcal{X})$ to denote the set of positive semidefinite, trace one operators (i.e., density operators) acting on \mathcal{X} .

A quantum channel Φ from Alice to Bob is a completely positive, trace-preserving linear map of the form

$$\Phi : \mathcal{L}(\mathcal{A}) \rightarrow \mathcal{L}(\mathcal{B}).$$

An important channel is the tracing operation, denoted by Tr , and mapping any input ρ to $\text{Tr}(\rho)$. When the tracing operation is applied to part of a multipartite system, it is called the partial trace, with a subscript specifying which system is being traced out. There exist several well-known characterizations of quantum channels. The first one we need is given by the Stinespring representation. A channel Φ is described as

$$\Phi(\rho) = \text{Tr}_{\mathcal{E}}(A\rho A^\dagger) \quad (1)$$

for some “environment” system \mathcal{E} and for some isometry $A \in \mathcal{L}(\mathcal{A}, \mathcal{B} \otimes \mathcal{E})$ (satisfying $A^\dagger A = \mathbb{1}$) known as an isometric extension of Φ . For any channel Φ , the isometric extension is uniquely determined up to left multiplication by an isometry acting on \mathcal{E} .

For a channel Φ with a Stinespring representation (1), the channel Ψ of the form $\Psi : \mathcal{L}(\mathcal{A}) \rightarrow \mathcal{L}(\mathcal{E})$ that is given by

$$\Psi(\rho) = \text{Tr}_{\mathcal{B}}(A\rho A^\dagger) \quad (2)$$

is called a *complementary channel* to Φ . Following the degree of freedom in the Stinespring representation, a complementary channel of Φ is uniquely determined up to an isometry to the final output. A channel Ψ that is complementary to Φ may be viewed as representing information that leaks to the environment when Φ is performed.

The second type of representation we need is a Kraus representation

$$\Phi(\rho) = \sum_{k=1}^N A_k \rho A_k^\dagger, \quad (3)$$

where the operators $A_1, \dots, A_N \in \mathcal{L}(\mathcal{A}, \mathcal{B})$ (called Kraus operators) satisfy

$$\sum_{k=1}^N A_k^\dagger A_k = \mathbb{1}. \quad (4)$$

The *coherent information* of a state $\rho \in \mathcal{D}(\mathcal{A})$ through a channel $\Phi : \mathcal{L}(\mathcal{A}) \rightarrow \mathcal{L}(\mathcal{B})$ is defined as

$$I_c(\rho; \Phi) = H(\Phi(\rho)) - H(\Psi(\rho)), \quad (5)$$

for any channel Ψ complementary to Φ , where $H(\sigma)$ denotes the von Neumann entropy of a density operator σ . Note that the coherent information is independent of the choice of the complementary channel Ψ . The coherent information of Φ is given by the maximum over all inputs

$$I_c(\Phi) = \max_{\rho \in \mathcal{D}(\mathcal{A})} I_c(\rho; \Phi). \quad (6)$$

The n -shot coherent information of Φ is $I_c(\Phi^{\otimes n})$. The *quantum capacity theorem* [Llo97, Sho02, Dev05] states that the quantum capacity of Φ is given by the expression

$$Q(\Phi) = \lim_{n \rightarrow \infty} \frac{I_c(\Phi^{\otimes n})}{n}. \quad (7)$$

The expression inside of the limit in (7) is nondecreasing in n , so the 1-shot coherent information $I_c(\Phi)$ provides a lower-bound on the quantum capacity of Φ .

The *qubit depolarizing channel* with noise parameter η , denoted by Φ_η , takes a qubit state $\rho \in \mathcal{D}(\mathbb{C}^2)$ to itself with probability $1 - \eta$, and replaces it with a random output with probability η :

$$\Phi_\eta(\rho) = (1 - \eta)\rho + \eta \frac{\mathbb{1}}{2}. \quad (8)$$

One Kraus representation of Φ_η is

$$\Phi_\eta(\rho) = (1 - \varepsilon)\rho + \frac{\varepsilon}{3}(\sigma_1 \rho \sigma_1 + \sigma_2 \rho \sigma_2 + \sigma_3 \rho \sigma_3), \quad (9)$$

where $\varepsilon = 3\eta/4$, and

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (10)$$

denote the Pauli operators. A Stinespring representation of Φ_η that corresponds naturally to this Kraus representation is

$$\Phi_\eta(\rho) = \text{Tr}_{\mathcal{E}}(A_\varepsilon \rho A_\varepsilon^\dagger) \quad (11)$$

for the isometric extension

$$A_\varepsilon = \sqrt{1 - \varepsilon} \mathbb{1} \otimes |0\rangle + \sqrt{\frac{\varepsilon}{3}}(\sigma_1 \otimes |1\rangle + \sigma_2 \otimes |2\rangle + \sigma_3 \otimes |3\rangle). \quad (12)$$

The complementary channel Ψ_η to Φ_η determined by this Stinespring representation is given by

$$\Psi_\eta(\rho) = \text{Tr}_{\mathcal{B}}(A_\varepsilon \rho A_\varepsilon^\dagger) = \begin{pmatrix} 1 - \varepsilon & \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_1, \rho\rangle & \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_2, \rho\rangle & \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_3, \rho\rangle \\ \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_1, \rho\rangle & \frac{\varepsilon}{3} & -\frac{i\varepsilon}{3}\langle\sigma_3, \rho\rangle & \frac{i\varepsilon}{3}\langle\sigma_2, \rho\rangle \\ \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_2, \rho\rangle & \frac{i\varepsilon}{3}\langle\sigma_3, \rho\rangle & \frac{\varepsilon}{3} & -\frac{i\varepsilon}{3}\langle\sigma_1, \rho\rangle \\ \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}\langle\sigma_3, \rho\rangle & -\frac{i\varepsilon}{3}\langle\sigma_2, \rho\rangle & \frac{i\varepsilon}{3}\langle\sigma_1, \rho\rangle & \frac{\varepsilon}{3} \end{pmatrix}. \quad (13)$$

We call this complementary channel the *epolarizing channel*. Note that when $\eta \approx 0$, the channel Φ_η is nearly noiseless, while Ψ_η is very noisy—and the opposite holds when $\eta \approx 1$.

We will use the expressions above to calculate a lower-bound on the coherent information $I_c(\Psi_\eta)$, which provides a lower-bound on the quantum capacity of the epolarizing channel Ψ_η .

Main result

Theorem 1. *Let Φ_η be the qubit depolarizing channel with noise parameter $\eta \in [0, 1]$. Any complementary channel to Φ_η has positive coherent information when $\eta > 0$.*

Proof of Theorem 1. The coherent information is independent of the choice of the complementary channel, so, it suffices to focus on the choice Ψ_η described in (13). Taking

$$\rho = \begin{pmatrix} 1 - \delta & 0 \\ 0 & \delta \end{pmatrix} \quad (14)$$

yields $\langle \sigma_1, \rho \rangle = 0$, $\langle \sigma_2, \rho \rangle = 0$, and $\langle \sigma_3, \rho \rangle = 1 - 2\delta$, and therefore

$$\Psi_\eta(\rho) = \begin{pmatrix} (1-\varepsilon) & 0 & 0 & \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}(1-2\delta) \\ 0 & \frac{\varepsilon}{3} & -\frac{i\varepsilon}{3}(1-2\delta) & 0 \\ 0 & \frac{i\varepsilon}{3}(1-2\delta) & \frac{\varepsilon}{3} & 0 \\ \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}}(1-2\delta) & 0 & 0 & \frac{\varepsilon}{3} \end{pmatrix}. \quad (15)$$

The entropy of $\Psi_\eta(\rho)$ is at least the entropy of the state

$$\xi = \begin{pmatrix} (1-\varepsilon) & 0 & 0 & \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}} \\ 0 & \frac{\varepsilon}{3} & \frac{\varepsilon}{3}(1-2\delta) & 0 \\ 0 & \frac{\varepsilon}{3}(1-2\delta) & \frac{\varepsilon}{3} & 0 \\ \sqrt{\frac{\varepsilon(1-\varepsilon)}{3}} & 0 & 0 & \frac{\varepsilon}{3} \end{pmatrix}, \quad (16)$$

which has eigenvalues $\{1 - \frac{2\varepsilon}{3}, 0, \frac{2\varepsilon}{3}(1-\delta), \frac{2\varepsilon}{3}\delta\} = \{1 - \frac{\eta}{2}, 0, \frac{\eta}{2}(1-\delta), \frac{\eta}{2}\delta\}$ and entropy

$$H(\xi) = \frac{\eta}{2} H_2(\delta) + H_2\left(\frac{\eta}{2}\right). \quad (17)$$

(A closed-form expression for the entropy of $\Psi_\eta(\rho)$ is not difficult to obtain, but the lower bound above has a simpler form and is sufficient to obtain the result.)

On the other hand,

$$\Phi_\eta(\rho) = \begin{pmatrix} (1-\eta)(1-\delta) + \frac{\eta}{2} & 0 \\ 0 & (1-\eta)\delta + \frac{\eta}{2} \end{pmatrix}, \quad (18)$$

and therefore

$$H(\Phi_\eta(\rho)) = H_2\left((1-\eta)\delta + \frac{\eta}{2}\right). \quad (19)$$

By the mean value theorem, one has

$$H_2\left((1-\eta)\delta + \frac{\eta}{2}\right) - H_2\left(\frac{\eta}{2}\right) = (1-\eta)\delta (\log(1-\mu) - \log(\mu)) \quad (20)$$

for some choice of μ satisfying $\eta/2 \leq \mu \leq (1-\eta)\delta + \eta/2$, and therefore

$$H(\Phi_\eta(\rho)) \leq H_2\left(\frac{\eta}{2}\right) + (1-\eta)\delta \log\left(\frac{2}{\eta}\right). \quad (21)$$

Therefore, the coherent information of ρ through Ψ_η is lower-bounded as follows:

$$I_c(\rho; \Psi_\eta) = H(\Psi_\eta(\rho)) - H(\Phi_\eta(\rho)) \geq H(\xi) - H(\Phi_\eta(\rho)) \geq \frac{\eta}{2} H_2(\delta) - (1-\eta)\delta \log\left(\frac{2}{\eta}\right). \quad (22)$$

The rightmost expression is strictly positive when

$$0 < \delta \leq 2^{-\frac{2(1-\eta)}{\eta} \log\left(\frac{2}{\eta}\right)}, \quad (23)$$

which completes the proof. \square

Comparisons with some well-known families of channels

The *qubit erasure channel* with noise parameter $\eta \in [0, 1]$, denoted by Ξ_η , takes a single qubit state $\rho \in \mathcal{D}(\mathbb{C}^2)$ to itself with probability $1 - \eta$, and replaces it by an error symbol orthogonal to the input space with probability η . The quantum capacity of the erasure channel is known and is given by $Q(\Xi_\eta) = \max(0, 1 - 2\eta)$ [BDS97].

We can relate the depolarizing channel, the erasure channel, and the epolarizing channel as follows. Let each of $\mathcal{A}, \mathcal{S}_1, \mathcal{S}_2, \mathcal{G}_1, \mathcal{G}_2$ denote a qubit system. Consider an isometry

$$A \in \mathcal{L}(\mathcal{A}, \mathcal{S}_1 \otimes \mathcal{S}_2 \otimes \mathcal{G}_1 \otimes \mathcal{G}_2 \otimes \mathcal{A})$$

acting on a pure qubit state $|\psi\rangle \in \mathcal{A}$ as

$$|\psi\rangle_{\mathcal{A}} \mapsto [|0\rangle\langle 0|_{\mathcal{S}_1} \otimes \mathbb{1}_{\mathcal{A}\mathcal{G}_1} + |1\rangle\langle 1|_{\mathcal{S}_1} \otimes \text{SWAP}_{\mathcal{A}\mathcal{G}_1}] |s\rangle_{\mathcal{S}_1\mathcal{S}_2} |\Phi\rangle_{\mathcal{G}_1\mathcal{G}_2} |\psi\rangle_{\mathcal{A}}, \quad (24)$$

where $|s\rangle = \sqrt{1-\eta}|00\rangle + \sqrt{\eta}|11\rangle$ and $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and where the subscripts denote the pertinent systems. The isometry can be interpreted as follows. System \mathcal{A} (the input space) initially contains the input state $|\psi\rangle_{\mathcal{A}}$, while a system \mathcal{G}_1 (which represents a “garbage” space) is initialized to a completely mixed state. The input is swapped with the garbage if and only if a measurement of the \mathcal{S}_1 system (which represents a “syndrome”) causes the state $|s\rangle$ of $\mathcal{S}_1\mathcal{S}_2$ to collapse to $|11\rangle$. Finally, each of the depolarizing, erasure, and the epolarizing channel can be generated by discarding a subset of the systems as follows:

$$\Phi_\eta(\rho) = \text{Tr}_{\mathcal{S}_1 \otimes \mathcal{S}_2 \otimes \mathcal{G}_1 \otimes \mathcal{G}_2}(A\rho A^\dagger), \quad \Xi'_\eta(\rho) = \text{Tr}_{\mathcal{S}_2 \otimes \mathcal{G}_1 \otimes \mathcal{G}_2}(A\rho A^\dagger), \quad \text{and} \quad \Psi'_\eta(\rho) = \text{Tr}_{\mathcal{A}}(A\rho A^\dagger). \quad (25)$$

To be more precise, the channel Ξ'_η in (25) is related to the channel Ξ_η described earlier by an isometry—for all relevant purposes, Ξ'_η and Ξ_η are equivalent. Likewise, Ψ'_η is equivalent to Ψ_η in (13). If we ignore the precise value of η , the systems \mathcal{A} and \mathcal{G}_1 carry qualitatively similar information. Furthermore, the additional garbage system \mathcal{G}_2 is irrelevant. So, the three families of channels are distinguished by which syndrome systems are available in the output: none for the depolarizing channel output, both for the epolarizing channel, and one for the erasure channel. These different possibilities cause significant differences in the noise parameter ranges for which the quantum capacity vanishes [BDS97, DSS98]:

$$\begin{aligned} Q(\Phi_\eta) &= 0 \quad \text{if} \quad 1/3 \leq \eta \leq 1, \\ Q(\Xi_\eta) &= 0 \quad \text{iff} \quad 1/2 \leq \eta \leq 1, \\ Q(\Psi_\eta) &= 0 \quad \text{iff} \quad 0 = \eta. \end{aligned} \quad (26)$$

In particular, when $\eta \approx 0$, the syndrome state carries very little information and only interacts weakly with the input—and yet having all shares of it in the output keeps the quantum capacity of the epolarizing channel positive. The syndrome systems therefore carry qualitatively significant information that is quantitatively negligible. To what extent this phenomenon is relevant to an understanding of the capacity of the depolarizing channel is a topic for further research.

We also note that the qubit amplitude damping channel (see [NC00]) has vanishing quantum capacity if and only if the noise parameter satisfies $1/2 \leq \eta \leq 1$, which is similar to the erasure channel (while the output only approaches a constant as $\eta \rightarrow 1$). The dephasing channel (see below) does not take the input to a constant for all noise parameters.

Extension to other channels

A mixed Pauli channel on one qubit can be described by a Kraus representation,

$$\Theta(\rho) = (1 - p_1 - p_2 - p_3) \rho + p_1 \sigma_1 \rho \sigma_1 + p_2 \sigma_2 \rho \sigma_2 + p_3 \sigma_3 \rho \sigma_3, \quad (27)$$

for $p_1, p_2, p_3 \geq 0$ satisfying $p_1 + p_2 + p_3 \leq 1$. For example, a *dephasing channel* can be described in this way by taking $p_1 = p_2 = 0$ and $p_3 \in [0, 1]$. In this case the quantum capacity is known to equal $1 - H_2(p_3)$, which is positive except when $p_3 = 1/2$. Any complementary channel of such a dephasing channel must have zero quantum capacity. If at least 3 of the 4 probabilities $(1 - p_1 - p_2 - p_3), p_1, p_2, p_3$ are positive, a generalization of our main result demonstrates that the capacity of a complementary channel of Θ has positive coherent information (see the appendix for a proof), so the phenomenon exhibited by the depolarization channel is therefore not an isolated instance. It is an interesting open problem to determine which mixed unitary channels in higher dimensions, meaning those channels having a Kraus representation in which every Kraus operator is a positive scalar multiple of a unitary operator, have complementary channels with positive capacity. (It follows from the work of [CRS08] that every mixed unitary channel with commuting Kraus operators is degradable, and therefore must have zero complementary capacity.)

Conclusion

We have shown that any complementary channel to the qubit depolarizing channel has positive quantum capacity unless its output is exactly constant. This gives an example of a family of channels whose outputs approach a constant, yet retaining positive quantum capacity. We also point out a crucial difference between the depolarizing channel and the related depolarizing and erasure channels. We hope these observations will shed light on what may or may not cause the quantum capacity of a channel to vanish.

Our work also rules out the possibility that Watanabe's results [Wat12] can be applied directly to show that the low-noise depolarizing channel has quantum capacity given by the 1-shot coherent information. While our results do not have direct implications to the quantum capacity of Φ_η , we hope they provide insights for further investigations into the quantum capacity of the low-noise depolarizing channel.

Acknowledgements

We thank Ke Li, Graeme Smith, and John Smolin for inspiring discussions on the depolarizing channel, and we thank the hospitality of the Physics of Information Group at IBM TJ Watson Research Center. We thank Frederic Dupuis, Aram Harrow, William Matthews, Graeme Smith, Mark Wilde, and Andreas Winter for a lively discussion concerning the depolarizing channel during the workshop, Beyond IID in Information Theory, 5-10 July 2015, and the hospitality of The Banff International Research Station (BIRS). This research was supported by NSERC, the Canadian Institute for Advanced Research, and the Canada Research Chairs Program.

References

- [BDE⁺98] Dagmar Bruß, David DiVincenzo, Artur Ekert, Christopher Fuchs, Chiara Macchiavello, and John Smolin. Optimal universal and state-dependent quantum cloning. *Physical Review A*, 57(4):2368, 1998.
- [BDS97] Charles Bennett, David DiVincenzo, and John Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78(16):3217, 1997.
- [CEM⁺15] Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. Unbounded number of channel uses may be required to detect quantum capacity. *Nature Communications*, 6, 2015.
- [CRS08] Toby Cubitt, Mary Beth Ruskai, and Graeme Smith. The structure of degradable quantum channels. *Journal of Mathematical Physics*, 49(10):102104, 2008.
- [Dev05] Igor Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005.
- [DSS98] David DiVincenzo, Peter Shor, and John Smolin. Quantum-channel capacity of very noisy channels. *Physical Review A*, 57(2):830–839, 1998.
- [HHH00] Paweł Horodecki, Michał Horodecki, and Ryszard Horodecki. Binding entanglement channels. *Journal of Modern Optics*, 47(2-3):347–354, 2000.
- [Llo97] Seth Lloyd. Capacity of the noisy quantum channel. *Physical Review A*, 55:1613–1622, 1997.
- [NC00] Michael Nielsen and Isaac Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.
- [Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413–1415, 1996.
- [Sha48] Claude Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 1948.
- [Sho02] Peter Shor. The quantum channel capacity and coherent information. Lecture notes, MSRI Workshop on Quantum Computation, 2002. Available online at <http://www.msri.org/realvideo/ln/msri/2002/quantumcrypto/shor/1/>.
- [SS12] Graeme Smith and John Smolin. Detecting incapacity of a quantum channel. *Physical Review Letters*, 108(23):230507, 2012.
- [Wat12] Shun Watanabe. Private and quantum capacities of more capable and less noisy quantum channels. *Physical Review A*, 85:012326, 2012.

A Extension of the main result to the mixed Pauli channel

Theorem 2. Consider the mixed Pauli channel on one qubit described by

$$\Theta(\rho) = p_0 \rho + p_1 \sigma_1 \rho \sigma_1 + p_2 \sigma_2 \rho \sigma_2 + p_3 \sigma_3 \rho \sigma_3, \quad (28)$$

where $p_0, p_1, p_2, p_3 \geq 0$, $p_0 + p_1 + p_2 + p_3 = 1$. If three or more of these probabilities are nonzero, then, any complementary channel to Θ has positive coherent information.

Proof of Theorem 2. The proof is similar to that of Theorem 1. We can assume without loss of generality that $p_0 \geq p_1 \geq p_2 \geq p_3$, by redefining the basis of the output space if necessary. A convenient choice of the isometric extension is

$$A = \sum_{i=0}^3 \sqrt{p_i} \sigma_i \otimes |i\rangle. \quad (29)$$

This gives a complementary channel Θ^c acting as

$$\Theta^c(\rho) = \text{Tr}_{\mathcal{B}}(A \rho A^\dagger) = \begin{pmatrix} p_0 & \sqrt{p_0 p_1} \langle \sigma_1, \rho \rangle & \sqrt{p_0 p_2} \langle \sigma_2, \rho \rangle & \sqrt{p_0 p_3} \langle \sigma_3, \rho \rangle \\ \sqrt{p_0 p_1} \langle \sigma_1, \rho \rangle & p_1 & -i\sqrt{p_1 p_2} \langle \sigma_3, \rho \rangle & i\sqrt{p_1 p_3} \langle \sigma_2, \rho \rangle \\ \sqrt{p_0 p_2} \langle \sigma_2, \rho \rangle & i\sqrt{p_1 p_2} \langle \sigma_3, \rho \rangle & p_2 & -i\sqrt{p_2 p_3} \langle \sigma_1, \rho \rangle \\ \sqrt{p_0 p_3} \langle \sigma_3, \rho \rangle & -i\sqrt{p_1 p_3} \langle \sigma_2, \rho \rangle & i\sqrt{p_2 p_3} \langle \sigma_1, \rho \rangle & p_3 \end{pmatrix}. \quad (30)$$

By hypothesis, $p_0 \geq p_1 \geq p_2 > 0$. We choose the following parametrization to simplify the analysis. Let $p_1 = p > 0$, $p_2 = \alpha p$ where $0 < \alpha \leq 1$, and $\eta' = 2(1 + \alpha)p$. We will see that the parameter η' enters the current proof in a way identical to the noise parameter η for the depolarizing channel in the proof of Theorem 1. Once again, we take

$$\rho = \begin{pmatrix} 1 - \delta & 0 \\ 0 & \delta \end{pmatrix} \quad (31)$$

so $\langle \sigma_1, \rho \rangle = 0$, $\langle \sigma_2, \rho \rangle = 0$, and $\langle \sigma_3, \rho \rangle = 1 - 2\delta$, and therefore

$$\Theta^c(\rho) = \begin{pmatrix} p_0 & 0 & 0 & \sqrt{p_0 p_3}(1 - 2\delta) \\ 0 & p_1 & -i\sqrt{p_1 p_2}(1 - 2\delta) & 0 \\ 0 & i\sqrt{p_1 p_2}(1 - 2\delta) & p_2 & 0 \\ \sqrt{p_0 p_3}(1 - 2\delta) & 0 & 0 & p_3 \end{pmatrix}. \quad (32)$$

The entropy of $\Theta^c(\rho)$ is at least the entropy of the state

$$\zeta' = \begin{pmatrix} p_0 & 0 & 0 & \sqrt{p_0 p_3} \\ 0 & p_1 & \sqrt{p_1 p_2}(1 - 2\delta) & 0 \\ 0 & \sqrt{p_1 p_2}(1 - 2\delta) & p_2 & 0 \\ \sqrt{p_0 p_3} & 0 & 0 & p_3 \end{pmatrix}. \quad (33)$$

The submatrix at the four corners give rise to the eigenvalues $\{p_0 + p_3, 0\} = \{1 - \frac{\eta'}{2}, 0\}$ as in the proof of Theorem 1. Meanwhile, the middle block can be rewritten as

$$\frac{\eta'}{2} \begin{pmatrix} \frac{1}{1+\alpha} & \frac{\sqrt{\alpha}}{1+\alpha}(1+2\delta) \\ \frac{\sqrt{\alpha}}{1+\alpha}(1+2\delta) & \frac{\alpha}{1+\alpha} \end{pmatrix} = \frac{\eta'}{2} \begin{pmatrix} \frac{1}{2} + \frac{\cos 2\theta}{2} & \frac{\sin 2\theta}{2}(1+2\delta) \\ \frac{\sin 2\theta}{2}(1+2\delta) & \frac{1}{2} - \frac{\cos 2\theta}{2} \end{pmatrix}, \quad (34)$$

where

$$\frac{1}{1+\alpha} = \cos^2 \theta = \frac{1}{2} + \frac{\cos 2\theta}{2}, \quad (35)$$

$$\frac{\alpha}{1+\alpha} = \sin^2 \theta = \frac{1}{2} - \frac{\cos 2\theta}{2}, \quad (36)$$

$$\frac{\sqrt{\alpha}}{1+\alpha} = \sin \theta \cos \theta = \frac{\sin 2\theta}{2}, \quad (37)$$

and $0 < \theta \leq \frac{\pi}{2}$. From equation (34), the eigenvalues of the middle block can be easily evaluated as $\frac{\eta'}{2} \{\frac{1}{2}(1+r), \frac{1}{2}(1-r)\}$ where

$$r^2 = \cos^2 2\theta + \sin^2 2\theta (1-2\delta)^2 = 1 - 4\delta \sin^2 2\theta + 4\delta^2 \sin^2 2\theta. \quad (38)$$

If we define the variable δ' to satisfy the equation $\delta(1-\delta) \sin^2 2\theta = \delta'(1-\delta')$, then, $r = 1 - 2\delta'$ and the two eigenvalues are $\{\frac{\eta'}{2}(1-\delta'), \frac{\eta'}{2}\delta'\}$.

Altogether, the spectrum of ξ' is $\{1 - \frac{\eta'}{2}, 0, \frac{\eta'}{2}(1-\delta'), \frac{\eta'}{2}\delta'\}$ which has the same form as the spectrum of ξ in the proof of Theorem 1, and the entropy of ξ' is analogous to (17),

$$H(\xi') = \frac{\eta'}{2} H_2(\delta') + H_2\left(\frac{\eta'}{2}\right). \quad (39)$$

On the other hand, $\Theta(\rho)$ has exactly the same expression as $\Phi_{\eta'}(\rho)$ and the entropy of $\Theta(\rho)$ is analogous to (19),

$$H(\Theta(\rho)) = H_2\left((1-\eta')\delta + \frac{\eta'}{2}\right). \quad (40)$$

Following arguments similar to the proof of Theorem 1, the coherent information of ρ through Θ^c is lower-bounded as follows:

$$I_c(\rho; \Theta^c) = H(\Theta^c(\rho)) - H(\Theta(\rho)) \geq H(\xi') - H(\Theta(\rho)) \geq \frac{\eta'}{2} H_2(\delta') - (1-\eta')\delta \log\left(\frac{2}{\eta'}\right). \quad (41)$$

We have a δ' -dependency in the first term and δ -dependency in the second term. However,

$$\delta(1-\delta) \sin^2 2\theta = \delta'(1-\delta'), \quad (42)$$

and $\sin^2 2\theta$ is a positive constant determined by $\alpha = p_2/p_1$, so for sufficiently small δ , the above equation is strictly positive. \square